Compendium On Standards for Cyber Security and Privacy in Information Technology

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
उपभोक्ता मामले, खाद्य और सार्वजनिक वितरण मंत्रालय, भारत सरकार
Ministry of Consumer Affairs, Food and Public Distribution, Government of India

Table of Contents

1. Introduction

With the rapid digitization of services and the increasing reliance on interconnected systems, cybersecurity has emerged as a critical area for governments, industries, and global institutions. As cyber threats become more sophisticated, the need for standardized frameworks to protect information and ICT infrastructures has grown significantly. Cybersecurity encompasses a wide range of considerations, including confidentiality, integrity, availability, accountability, privacy, resilience and trust in digital systems.

The Bureau of Indian Standards (BIS), India's National Standards Body, plays a leading role in developing cybersecurity standards. Through its LITD 17 committee, BIS mirrors ISO/IEC JTC 1/SC 27—the international committee dedicated to Information security, cybersecurity and privacy protection. JTC 1/SC 27 develops international standards addressing the protection of information and ICT systems through generic methods, guidelines, and techniques.

These standards specify security requirements, guide information and ICT security management through Information Security Management Systems (ISMS), cryptographic and other technical measures. These standards also address identity management, biometrics, privacy, criteria for conformance assessment, auditing, and security evaluation.

These standards aim to address confidentiality, integrity and availability as major aspects for cyber security.

We extend our sincere appreciation to the experts, stakeholders, and organizations whose contributions have shaped this compendium. We trust that this document will support the widespread adoption of standardized cybersecurity practices and enhance India's role as a proactive leader in cybersecurity efforts.

2. Cyber Security Standardization -National and global efforts

LITD 17 committee of Bureau of Indian Standards is the for Standardization in the area of Information security and privacy. There are some other committee as well which develops standards related to the aspects of cyber security. Other committees are

ETD 18, Industrial Process Measurement and Control, Sectional Committee

SSD 3 Banking and Financial Services

LITD 10 Power System Control and Associated Communications

More details on BIS committees are provided at BIS Technical Committees

Cyber security being a technology which transcends boundaries, the LITD 17 committee works in sync with the International standardization work of ISO/IEC JTC 1/SC 27, committee of International Organization for Standardization (ISO) and International Electro-Technical

Commission (IEC). Experts from 91 countries, including India participate in the work of this committee. More details about ISO/IEC JTC 1/SC 27 committee on cybersecurity and privacy are provided in ISO/IEC JTC 1/SC 27

BIS Committee, LITD 17 on Information security and privacy is the national mirror committee of this important international cyber security and privacy committee (JTC 1/SC 27). Only the members represented on BIS committee are eligible to participate and contribute towards international standardization efforts in SC 27. BIS's endeavor is to have strong presence and participation of Indian experts in SC 27 so as to ensure that national priorities and requirements are incorporated while bringing out international standards. This ensures seamless adoption and implementation of the international standards within the country.

3. Cyber Security and Privacy in IT – Key Topics of Standardizations

- Information Security Management Systems (ISMS)
- Cryptographic Techniques and Key Management
- Evaluation of IT Security
- Data Privacy and Protection
- Domain specific security standards

3.1 Information Security Management Systems (ISMS)

1. **IS/ISO/IEC 27000:2018 Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary (First Revision)**

   This document provides an overview of Information Security Management Systems (ISMS), offering key terms and definitions commonly used across the ISMS standards family. It serves as a foundational guide for implementing and maintaining ISMS framework. It explains the purpose and structure of ISMS standards, which include requirements, guidance, and sector-specific practices to help organizations protect their information assets and prepare for independent assessments.

2. **IS/ISO/IEC 27001:2022 Information Security Management Systems – Requirements (Second Revision)**

   This document outlines requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of information.

3. **IS/ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection – Information security controls. Implementation guidance**

   This document offers guidance for organizations to implement and manage information security controls within an ISMS based on ISO/IEC 27001. There are 93 controls listed in 27002 and these categorized as organizational controls, people controls, physical

controls and technological controls.

4. **IS/ISO/IEC 27003:2017 Guidance for the implementation of ISMS**

   This document offers guidance on implementing the requirements of ISO/IEC 27001:2013 for establishing and improving an Information Security Management System (ISMS). It explains key ISMS components like risk assessment, policy development, roles, planning, and continual improvement.

5. **IS/ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of ISMS**
   This document outlines specific requirements and guidance for organizations that audit and certify for ISMS.

6. **IS/ISO/IEC 27033 Series** Information technology — Security techniques — Network security

   This series of standards provides comprehensive guidance on network security. These provides an overview of network security concepts, risk assessment, and controls. These also gives guidelines for planning, designing, implementing, and documenting network security.
   These documents also detail threats, threat analysis, design techniques, and control issues for various network scenarios, using security gateways like firewalls and intrusion protection systems. These documents provide guidance to secure Virtual Private Networks (VPNs), securing IP wireless networks

7. **IS/ISO/IEC 27034 series Application security**

   ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications.

   This series of standards It introduces concepts like Application Security Controls (ASCs), which are specific measures to prevent security weaknesses, and frameworks such as the Organization Normative Framework (ONF) and Application Normative Framework (ANF) to manage security at organizational and application levels, respectively.

8. **ISO/IEC 27035 series Information security incident management**

   This series provides comprehensive guidance on information security incident management outlining fundamental principles and processes for managing incidents, emphasizing preparation, detection, response, and learning to minimize business impact, applicable to all organizations.

9. **IS/ISO/IEC 27036 series Cybersecurity – Supplier relationships**

   The ISO/IEC 27036 series provides comprehensive guidance on managing information

security risks in supplier relationships. These documents introduce key concepts, shared responsibilities for secure collaboration, sets fundamental security requirements for all types of supplier-acquirer relationships, emphasizing visibility, risk assessment, trust boundaries, and lifecycle-based risk management and focusing on defining, implementing, and improving security practices. These documents also address cloud service relationships.

3.2. Cryptographic Techniques and Key Management

10. IS/ISO/IEC 11770 Series Information Technology - Security Techniques - Key Management

This series is a set of standards that define mechanisms for key management for the secure handling of cryptographic keys used to protect information. It consists of seven parts, each focusing on different techniques and environments for establishing and managing cryptographic keys like *mechanisms for symmetric techniques and asymmetric techniques, Mechanisms Based on Weak Secrets*

11. IS/ISO/IEC 18033 series Encryption algorithms

The ISO/IEC 18033 series provides standardized definitions and guidance on encryption systems used to ensure the confidentiality of data. It introduces the fundamental principles of encryption, where plaintext is transformed into cipher text using an algorithm and a key, ensuring that the original data cannot be understood without proper decryption. The series specifies symmetric encryptions, asymmetric encryption, block ciphers, stream ciphers and homomorphic encryption systems.

12. IS/ISO/IEC 29192 series Lightweight cryptography

IS/ISO/IEC 29192 series is a multi-part standard for lightweight cryptography tailored to resource-constrained environments like RFID, smart cards, and sensor networks.

These standards common terminology, security, and implementation requirements. These documents provide specifications for implementing lightweight cryptographic mechanisms, including block ciphers, stream ciphers, asymmetric techniques, hash functions, message authentication codes (MACs), and authenticated encryption methods

Algorithms, mechanisms like *PRESENT, CLEFIA, LEA, Enocoro, Trivium, authenticated lightweight key exchange (ALIKE) mechanism, cryptoGPS , LightMAC, Tsudik's keymode, Chaskey-12, ACORN, PHOTON, SPONGENT etc.* are specified in this series of standards.

13. IS/ISO/IEC 19790:2025 Security requirements for cryptographic modules.

This document provides recommendations and checklists to support the secure deployment and operational testing of cryptographic modules. It guides operational testers in assessing module installation, configuration, key management, authentication credentials, and potential vulnerabilities.

3.3. Evaluation of IT Security

14. IS 14990 Series Evaluation Criteria for IT Security

This series is aligned with ISO/IEC 15408 (Common Criteria) and provides a structured framework for IT security evaluation across five parts. These parts describe concepts and evaluation criteria like security functional components, security assurance components, Pre-defined packages of security requirements.

These standards enable consistent specification, assessment, and assurance of IT security and privacy, supporting reliable evaluation and certification.

15. IS 15671:2024 Methodology for IT security evaluation

This document is aligned with ISO/IEC 18045. It provides guidance for evaluators conducting IT security evaluations under the ISO/IEC 15408 (Common Criteria) series. It defines the minimum required actions during evaluations and is mainly intended for evaluators and certifiers, with secondary users including developers and protection profile authors.

16. IS/ISO/IEC 19896 series Requirements for the competence of IT security conformance assessment body personnel

The IS/ISO/IEC 19896 series defines the minimum competence requirements for individuals like of testers, evaluators and validators involved in IT product security evaluations, conformance testing, certification, and validation. It provides a structured framework of knowledge, skills, and qualifications necessary to ensure the reliability, consistency, and comparability of security assessments across different schemes and geographies.

3.4. Data Privacy and Protection

17. IS 17428 Series Data Privacy Assurance

The IS 17428 series on Data Privacy Assurance comprises of two parts. Part 1 defines mandatory requirements for establishing and managing a Data Privacy Management System (DPMS) for organizations processing personal data electronically. Part 2 provides guidance for implementation of part 1.

18. **IS/ISO/IEC 29100:2024 Information technology — Security techniques — Privacy framework**

    This document presents a high-level privacy framework for protecting personally identifiable information (PII) in information and communication technology (ICT) systems. It provides common terminology, privacy principles, defines key actors and their roles in PII processing.

19. **ISO/IEC 29101:2018 Information technology — Security techniques — Privacy architecture framework**

    This document outlines a high-level privacy architecture framework for ICT systems that process personally identifiable information (PII). It offers a consistent approach for implementing privacy controls, guiding the design and development of systems that protect PII through controlled processing, access, and transfer. The document identifies key architectural concerns, system components, and views, and is intended for all entities involved in developing or managing ICT systems that interact with PII.

3.5. Domain specific security standards

20. **IS/ISO/IEC 27400:2022 Cybersecurity – IoT security and privacy guidelines**

    This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

21. **IS/ISO/IEC 27402: 2023 Cybersecurity - IoT Security and Privacy - Device Baseline Requirements**

    This document establishes baseline cybersecurity and privacy requirements for Internet of Things (IoT) devices.

22. **IS/IEC 62351 Series Power Systems Management and Associated Information Exchange Data and Communication Security**

    This series of documents gives detailed advice on protecting energy management systems and on the secure exchange of energy-related data. This series addresses system architecture and identifies a series of effective countermeasures that can be applied to commonly used protocols to protect the confidentiality, integrity and availability of data. It helps to protect against malicious attacks and disruptions to the power supply, ensuring a reliable and resilient power grid.

23. **IS/IEC 62443 series Industrial Communication Networks security**

Industrial Automation and Control Systems (IACS) cybersecurity. It is designed to protect industrial networks (like those used in manufacturing, energy, water treatment, etc.) from cyber threats. This series is primarily used for Operational Technology (OT) security and Industrial IoT (IIoT).

24. IS 15402 series Personal Identification Number (PIN) Management and Security

This series of standards defines fundamental principles for PIN management, specifies encryption algorithms and modes for protecting PINs during transmission, Outlines requirements for banks, processors, and service providers who manage or process PINs. These also provides requirements for PIN Handling in eCommerce for Payment Transactions, for cardholder verification mechanisms in open network environments, such as online or mobile transactions.

25. IS 17737 series Mobile device security

This series of documents provides overview. of mobile device technology and ecosystem. These documents identify high-level security risks and defines security characteristics and control requirements addressing threats to the mobile device technology stack, including hardware, firmware, OS, and pre-installed apps. These documents also define security levels, the associated requirements, methodology and approach for assessing and evaluating mobile device security based on the security levels